Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology[1]

before the
House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security

Oversight Hearing on Implementation of the USA PATRIOT Act: Section 212

May 5, 2005

Chairman Coble, Rep. Scott, Members of the Committee, thank you for the opportunity to testify today. As we said when we testified at an earlier hearing in this series, CDT commends the Subcommittee and the full Committee leadership for undertaking these important hearings on the PATRIOT Act. The members of this Subcommittee have devoted considerable time to understanding the provisions of the PATRIOT Act and how they fit within the context of the electronic surveillance laws. From this kind of detailed, objective inquiry, we can attain the balance that was left aside in the haste and emotion of the weeks after 9/11.

CDT's main point in these hearings is that while, of course, the law needs to keep pace with changing technology to ensure that government agencies have access to information to prevent crime and terrorism, those government powers will be no less effective – indeed will be more effective -- if they are subject to checks and balances. The law needs to keep pace with changing technology not only to ensure reasonable government access but also to protect privacy, as technology makes ever larger volumes of information available for the government to acquire from third parties, without satisfying traditional Fourth Amendment standards of a warrant and notice. The PATRIOT Act addressed only one side of this equation, making government access easier without counterbalancing privacy improvements. Now is the time for Congress to finish the job and address the privacy side of the equation.

In CDT's view, there is not a single kind of record or communication covered by the PATRIOT Act to which the government should be denied access. The question before us – and it is one of the most important questions in a democratic society – is what checks and balances should apply to government surveillance powers. With respect to

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

the particular PATRIOT section at issue in today's hearing, those time-honored checks and balances should include:

- First, as a general rule, individuals should have notice when the government acquires their communications.

- Second, surveillance techniques should be subject to judicial review, preferably prior judicial approval, but if that is not possible, judicial review after the fact, with sanctions for abuse of the authority.

- Finally, government surveillance needs to be subject to Congressional oversight and some public accountability, including through routine statistical reports.

Section 212 of the PATRIOT Act fails to include these checks and balances.

Prevention of Terrorism Does Not Require Suspension of Standards and Oversight

At the outset, let me repeat some basic points on which I hope there is widespread agreement:

- Terrorism poses a grave and imminent threat to our nation. There are people -- almost certainly some in the United States -- today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.
- The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to conduct electronic surveillance, carry out physical searches effectively, and obtain transactional records or business records pertaining to suspected terrorists.
- These authorities, however, must be guided by the Fourth Amendment and subject to Executive and judicial controls as well as legislative oversight and a measure of public transparency.

Section 212 – Emergency disclosures of email and other stored communications

This hearing focuses on Section 212 of the PATRIOT Act, relating to emergency disclosures of email and other stored communications. Section 212, like several other electronic surveillance provisions in the PATRIOT Act, has no direct connection with terrorism. It applies not to intelligence investigations, but to all criminal cases.

Section 212 allows the government to tell an Internet Service Provider (ISP) or telephone company that there is an emergency and the ISP or telephone company can then disclose your email, voicemail, or other stored communications without even a

subpoena, let alone a warrant, and never tell you so that you never have an opportunity to challenge the disclosure.

-- Increasing storage of communications under control of third parties threatens traditional Fourth Amendment protections

In our prior testimony, we described the "storage revolution" that is sweeping the field of information and communications technology. ISPs and other service providers are offering very large quantities of online storage for email, documents, and, in the latest emerging services, for voicemail. Increasingly, ordinary citizens are storing information not in their homes but on computer servers, under the control of service providers who can voluntarily or under compulsion disclose the communications and never have to tell the subscribers that their privacy has been compromised.

This technological revolution, coupled with exceptions like Section 212, is eroding Fourth Amendment protections. Traditionally, when records were stored locally, even if there was an emergency justifying an exception to the warrant requirement, you would normally receive notice of the search of your home or office. Yet individuals are never told of Section 212 disclosures unless the evidence is introduced against them at trial. Ironically, under 212, if the email of an innocent person is disclosed by mistake, that person will probably never be advised that the government has obtained their private data.

-- "Off the books" surveillance

Section 212 represents another in a steadily growing series of exceptions to the protections of the electronic communications privacy laws. (The computer trespasser provision of Section 217 is another example.) Section 212 and similar provisions essentially allow "off the books surveillance" – they define certain government interceptions not to be interceptions, and certain disclosures to the government not to be disclosures.

Once an access to communications or data is excluded from the coverage of the surveillance laws, not only is it not subject to prior judicial approval, but there are no time limits on the period covered by the surveillance or disclosure, no minimization requirement, no report back to a judge, no notice to the persons who are surveilled unless and until the government introduces the evidence against them in a criminal trial, no suppression rule for violating the statute's standards (no suppression remedy at all if the information is deemed to be outside the protection of the Fourth Amendment), and no reports to Congress and the public.

Emergency exceptions are sometimes reasonable, although in an age when warrants can be obtained by telephone or fax and presumably even by email, see Federal Rule of Criminal Procedure 41(d)(3), and when every court should have a duty judge available by cell phone or Blackberry 24 hours a day, emergency exceptions to judicial oversight should be extremely rare. And they should be subject to checks and balances.

-- The potential for government exaggeration of the facts

The crucial thing to recognize about Section 212 is that the information about the emergency will often come from a government agent. Rather than going to a judge and getting a warrant, even if time and technology permitted it, Section 212 permits a government agent to go to a service provider, say there is an emergency, and if the service provider reasonably believes there is (even if the government agent was exaggerating), the service provider can disclose the records with no liability and no notice to the subscriber. Surely, this is an invitation to cutting corners, if not more cynical forms of abuse. Notice also how placing the reasonable belief on the part of the service provider diffuses responsibility: the stored records provisions to which this exception was added has no suppression rule for evidence improperly obtained, and it does not appear that the civil action and administrative discipline provisions of 18 U.S.C. 2707 would apply to agents who even intentionally mislead a service provider about the existence of an emergency.

Other parts of Section 212 are non-controversial: It rearranged sections 2702 and 2703 of title 18 so that section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers compulsory disclosures. Second, an amendment to the new subsection 2702(c)(3) clarifies that service providers have the statutory authority to disclose non-content records to protect their rights and property.

The language of Section 212 covering emergency disclosures of the content of communications was rewritten by the act creating the Department of Homeland Security. In some ways the new language is narrower than the PATRIOT language, while in other ways it is broader (it allows disclosure not only to law enforcement but to any government entity), but our concerns and recommendations about checks and balances pertain to the new language as well. Also, an uncodified provision of the Homeland Security Act required government entities obtaining the contents of communications under the new emergency exception to report to the Attorney General and the Attorney General to file a one-time report to Congress in November 2003 on the use of the authority. Someone needs to look for that report.

-- Recommended amendments to establish checks and balances

Checks and balances should be added to Section 212.

- The person whose privacy has been compromised should be notified that his information has been disclosed to the government. This is especially important in cases of mistake – where the government obtains records on the wrong person, that person should be notified.
- There should be a statutory remedy for abuse, barring the government from using information if it had mislead the service provider into believing there was an emergency. An additional or alternative protection would be to make it illegal for a government official to intentionally or recklessly mislead a service provider as to the

existence of an emergency. Coupled with notice, this could provide a reasonable remedy to persons whose privacy was needlessly invaded.

- To permit ongoing oversight, emergency disclosures of stored communications to the government should be reported to Congress in annual, public statistical reports.

The Big Picture: Protections for Privacy Should Be Updated in Light of Changing Technology

As CDT has noted before, many of the changes in the PATRIOT Act appear small in isolation. However, no consideration has been given in almost five years to other, long-recognized changes that need to be made to strengthen the privacy protections of the electronic surveillance laws, including:

- extending Title III's statutory suppression rule to electronic communications, a change even the Justice Department once supported;
- increasing the standard for pen registers and trap and trace devices, to give judges meaningful oversight, a change the full Judiciary Committee supported in 2000;
- eliminating the distinctions between opened and unopened email and between relatively fresh and older email, by bringing all stored email under a warrant standard, another change the Committee supported in 2000;
- establishing a probable cause standard for access to location information, a change this Committee also supported in 2000;
- requiring reporting on access to email, also supported by the Committee in 2000.

With this context in mind, it is easier to see why even some of the minor changes in the PATRIOT Act draw concern, for they are part of a steady stream of uni-directional amendments that are slowly eroding the protections and limits of the electronic privacy laws.

Conclusion

CDT supports the Security and Freedom Enhancement (SAFE) Act, a narrowly tailored bipartisan bill that would revise several provisions of the PATRIOT Act. It would retain all of the expanded authorities created by the Act but place important limits on them. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

We look forward to working with this Subcommittee and the full Committee as you move forward in seeking to establish some of the checks and balances that were left behind in the haste and anxiety of October 2001.

For more information, contact: Jim Dempsey (202) 637-9800 x112